وزارت تحصیلات عالی
پوهنتون رنا
پوهنځی کمپیوتر ساینس
دیپارتمنت انجینری نرم افزار
کورس پالیسی

Subject	Network Security
Teacher Name	Baitullah Malakhil
Phone Number	0788794000
Semester	7th
Subject Code	CS.IT.0743
Number of Credit	3
Prerequisite Subject	Network Fundamental
Learning Objective	1. Understand network security principles. 2. Identify common network threats. 3. Implement security best practices. 4. Secure network infrastructure components. 5. Explore authentication methods. 6. Study encryption techniques. 7. Analyze network monitoring. 8. Develop incident response skills. 9. Assess vulnerabilities and risks. 10. Harden network devices. 11. Configure firewalls and intrusion detection. 12. Stay current with emerging threats.
Teaching Methodology	Conceptual + Theoretical
Date	23 Sep 2023
Course Assessment	Daily evaluation and oral assessment Mid Term 30% Assignment 10% Quiz 10% Final Term 50%
Reference Book	1. "Network Security Essentials" by William Stallings 2. "Principles of Information Security" by Whitman & Mattord 3. "Network Security" by Kaufman, Perlman & Speciner

جدول زمان بندی جلسات در طول سمستر				
Weeks	**Topics**	**Objectives**	**Teaching and Training Activities**	**Evaluation Method**
1	• Introduction • What is security • Some examples • Security Attack categories • Security violation categories • Security Measure levels	• Grasp security fundamentals. • Recognize security examples. • Categorize attack and violation types. • Understand security measures. •	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture • assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
2	Principles of Network security • The interrelated components of the computing environment • Network security models (the CIA triad, the star model, the Parkerian hexad) • Variations on a theme: computer security, information security, and information assurance	• Understand computing environment components and their relevance to network security. • Explore network security models like the CIA triad, star model • Differentiate between computer security, information security, and information assurance concepts.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
3	Why Security is difficult to achieve? • How Security become an issue? • Threat Modeling • Risk assessment	• Grasp the challenges in achieving security. • Identify factors that elevate security as an issue. • Learn about threat modeling techniques. • Understand the significance of risk assessment in security.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.

4	How to get Secure? • 3 Aspects of Security • Points to remember • Related topics	• Understand the three key aspects of security. • Internalize important points to enhance security. • Explore related topics and their relevance to security measures.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
5	Cryptography & Hash Algorithm • Classification of Cryptography • History of Cryptography • Basic Terminology of Cryptography	• Classify cryptography techniques. • Explore cryptography's historical evolution. • Learn fundamental cryptography terminology.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
6	Symmetric cryptography • Caesar cipher • Monoalphabetic cipher • One-time pad cipher • Rail fence cipher • Product cipher	• Grasp symmetric cryptography principles. • Study Caesar, monoalphabetic , and one-time pad ciphers. • Explore Rail fence and product ciphers in symmetric cryptography.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
7	Modern symmetric cipher • Block cipher • Stream cipher • Festal cipher	• Grasp modern symmetric ciphers. • Differentiate between block and stream ciphers. • Understand the Festal cipher in modern cryptography.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.

			• close: summarizing the lecture assignments	
8	Electronic Code Book • Cipher Block Chaining • Modular Mathematics • Method to Encrypt messages	• Understand ECB encryption mode. • Grasp CBC encryption mode. • Learn modular mathematics in cryptography. • Master methods for encrypting messages.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
9	• RSA Public Key System • Trapdoor • Deffie-Hellman Algorithm	• Grasp the RSA Public Key System. • Understand the concept of a trapdoor function. • Learn about the Deffie-Hellman Algorithm for key exchange.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
10	Authentication • Password Based • Address Based • Cryptographic Based	• Study password-based authentication. • Understand address-based authentication. • Explore cryptographic-based authentication methods.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
11	• Hash Algorithm/Message Digest • MD2 • MD4 •	• Grasp hash algorithms and message digests. • Examine MD2 hashing. • Explore MD4 hashing for	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.

		message integrity and security.	• Lecture presentation • Open discussion • close: summarizing the lecture assignments	
12	• Digital Signature • Trusted Intermediaries • Key Distribution Protocol	• Grasp digital signatures in secure communication • Understand the role of trusted intermediaries. • Learn key distribution protocols for secure key exchange.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
13	• Digital Certificate • Certification Authority • Certificate Revocation List(CRL) • Overview of Microsoft Certificate Server • Certificate Server Configuration • Certificate Server features • Certificate Sever Architecture	• Grasp digital certificates' role in security. • Understand the function of a Certification Authority (CA). • Learn about Certificate Revocation Lists (CRLs). • Gain an overview of Microsoft Certificate Server and its components.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
14	• Email • Email architecture • Threats • PGP	• Grasp email basics. • Explore email architecture. • Recognize email threats. • Learn about PGP for email security.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.
15	• IPsec • Firewalls	• Grasp IPsec for network	• AO-Asking the students	• feedback • Q&A

		security. • Understand the function of firewalls in network protection.	about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• Discussion • Application • Reflection. Summative: 1Q for final exam.
16	• Packet Filter • Application level Gateway • Hybrid • Privacy Enhance Mail (PEM) • Structure of PEM • Source Authentication and Integrity Protection	• Grasp packet filters in network security. • Explore application-level gateways. • Learn about hybrid security solutions. • Study Privacy Enhanced Mail (PEM) for email security. • Examine PEM's structure.	• AO-Asking the students about the previous topic. • • Specifying the objectives of today lesson • Lecture presentation • Open discussion • close: summarizing the lecture assignments	• feedback • Q&A • Discussion • Application • Reflection. Summative: 1Q for final exam.

قرار شرح فوق کورس پالیسی مضمون (Network Security) طبق کریکولم ترتیب وصحت است

امضاء استاد

تائیدی آمر دیپارتمنت

کورس پالیسی مضمون (Network Security) در جلسۀ شورای علمی پوهنځی مؤرخ 23 Sep 2023 مورد بررسی قرار گرفت وبه اتفاق آراء تصویب گردید ودر کتاب جلسات به شمارۀ پروتوکول ( ) قید گردید.

نام وامضاء رئیس پوهنځی

مهر پوهنځی